EEN GOED GESPREK

WAAROM DEZE KAARTJES?

Dreigingsbeeld informatiebeveiliging 2023 → 2024

Meer ransomware met destructievere gevolgen

Steeds meer en ernstiger kwetsbaarheden in software

Gevaren in ketens uit het zicht

- De dreiging voor Nederlandse gemeenten neemt toe (IBD Dreigingsbeeld ‘23-‘24).
- De Informatiebeveiligingsdienst (IBD) ondersteunt de gemeentesecretaris (GS) bij het invullen van zijn rol en verantwoordelijkheid als hoeder van de continuïteit van de gemeentelijke dienstverlening.
- Het is hiervoor van belang dat de GS, de CISO, de FG en de PO elkaar goed weten te vinden.
- Met deze gesprekskaartjes verwerft de GS snel basiskennis en weet hij of zij welke vragen te stellen aan adviseurs en aan proceseigenaren. Dit helpt de GS ook het belang van informatiebeveiliging & privacy (IB&P) uit te leggen in de organisatie (management en medewerkers) en aan het bestuur.

DE IBD ONDERSTEUNT OOK DE GS

- Hulp en advies bij incidenten aan de GS als voorzitter van het crisisteam. Denk aan: duiding van technische rapportages en adviezen van de eigen organisatie en derden, advies over de gevolgbestrijding, de herstelaanpak, communicatie en woordvoering. De IBD is een vertrouwde partij, met veel praktijkervaring, zonder eigenbelang.
- Oefenen met incidenten (table top oefening op basis van recente, echte incidenten, op maat voor uw organisatie).
- 'Kaartje voor in de meterkast' met daarop essentiële informatie ter voorbereiding op een crisis.
- Toegankelijke informatie over IB&P, zoals:
  - 'Dreigingsbeeld Nederlandse gemeenten' met aandachtspunten voor de weerbaarheid van de gemeente;
  - presentaties/ workshops over het onderwerp.
- Bijdragen aan: leergang / opleidingen, denk aan sprekers en ondersteuning vanuit de IBD om het onderwerp te agenderen in de organisatie. En aan leergang/ lunchuurtjes/ presentaties voor de VGS voor in kringen.

TIPS ALGEMEEN

- Het is van belang dat de CISO, de FG en de PO de GS gemakkelijk weten te vinden (en andersom; dat de GS deze functionarissen weet te vinden) en hier een laagdrempelige ingang hebben.
- Maak als GS een vaste terugkerende afspraak met de CISO, de PO en de FG, bijvoorbeeld eens per kwartaal.
- Uitbesteden vraagt om governance van de gemeente en een heldere taakverdeling; dit is belangrijk bij incidenten en bij verstoringen.
- Zorg dat ten minste de basisbeveiligings- en gegevensbeschermingsprocessen ingericht zijn.
- De mens is en blijft de zwakste schakel. Zorg voor een continu bewustwordingsprogramma, betrek alle gemeentemedewerkers daarbij en controleer of dit gebeurt.
- Stimuleer samenwerken met andere gemeenten op het gebied van cybersecurity en privacy.
- Spreek proceseigenaren aan op hun verantwoordelijkheden met betrekking tot cybersecurity en privacy.
- Zet cybersecurity en privacy op de agenda bij alle overleggen.
- Zorg ervoor dat Bedrijfscontinuïteitsplannen up to date zijn en dat deze worden geoefend. De IBD heeft een tabletop oefening ontwikkeld die de GS kan inzetten om dit te toetsen.

TIPS ALGEMEEN

Posities van de verschillende functionarissen binnen IB&P

De FG:

- is onafhankelijk;
- houdt toezicht op de hele organisatie, inclusief de GS en het bestuur.

De CISO en de PO:

- hebben een 2e lijns- (advies)rol;
- moeten goed hun adviesrol kunnen innemen richting de GS en proceseigenaren (bijvoorbeeld ten aanzien van de vraag of proceseigenaren IB&P goed borgen), van belang dat zij dit goed en redelijk onafhankelijk kunnen doen;
- leggen verantwoording af aan de GS.

Proceseigenaren:

- zijn verantwoordelijk voor het borgen van IB&P binnen hun processen en het mitigeren van de risico's.

1 MANAGEMENT VERANTWOORDELIJKHEDEN

Wie is er nu van IB&P? De FG, de CISO, de PO of iemand anders?

Bijna alle gemeenten hebben een CISO (chief information security officer), een FG (Functionaris voor Gegevensbescherming) en een PO (privacy officer). Dat betekent niet dat Informatiebeveiliging & Privacy (IB&P) automatisch is geregeld.

Proceseigenaren zijn verantwoordelijk voor de bescherming van de informatie die zij verwerken, niet de CISO, de FG of de PO. Proceseigenaren moeten afspraken maken met de CISO en de PO over de aandachtspunten binnen de domeinen waar zij verantwoordelijk voor zijn (PIOFAH: personeel, informatie, organisatie, financiën, automatisering en huisvesting). Hier horen eigenlijk 2 letters bij: de S van security en de P van privacy. Ook hierover moeten managementafspraken worden gemaakt.

Het is aan de GS om proceseigenaren hier op aan te spreken. Als de gemeente niet duidelijk benoemt wie de proceseigenaren zijn, als zij geen verantwoording moeten afleggen en niet worden gecontroleerd, is de kans groot dat proceseigenaren IB&P niet serieus nemen. Daardoor staat u als GS met 1-0 achter en loopt uw gemeente risico's.

1 MANAGEMENT VERANTWOORDELIJKHEDEN

Vragen die een GS moet stellen over informatiebeveiliging & privacy (IB&P) aan managers binnen de gemeente:

- Zijn de verantwoordelijkheden over IB&P benoemd in de omschrijving van alle managementfuncties binnen de gemeente?
- Waar staan deze IB&P-verantwoordelijkheden op de agenda? Worden ze in alle managementoverleggen besproken?
- Is IB&P een vast onderdeel van managementrapportages?
- Worden de IB&P procesrisico's besproken tijdens de managementoverleggen, en met de PIOFAH-proceseigenaren?
- In hoeverre is IB&P onderdeel van de beoordelingscyclus van medewerkers en management en/of de werkafspraken?
- Hoe vaak oefent uw gemeente met uitwijk- en calamiteitenplannen op het gebied van IB&P (datalekken, inbraak, gijzelsoftware)?

2 INFORMATIEBEHOEFTE GS

De CISO van de gemeente:

- moet de directie adviseren hoe zij de verantwoordelijkheid voor digitale veiligheid concreet kan oppakken.
- moet met een afwegingskader komen: welke prioritering is belangrijk en waarom? Welke keuzes zijn er dan nog te maken?

De PO van de gemeente:

- moet de directie adviseren hoe zij de verantwoordelijkheid voor privacy concreet kan oppakken.
- moet met een afwegingskader komen: welke prioritering is belangrijk en waarom? Welke keuzes zijn er dan nog te maken?

De uitdagingen:

- CISO, PO en GS komen vaak uit verschillende vakgebieden en spreken een andere taal.
- Niet alle GS zijn even benaderbaar voor een CISO of de PO. De CISO en PO zitten soms opgesloten in een hiërarchische structuur, waardoor toegang tot de GS niet laagdrempelig is. Ook komt het voor dat de GS onvoldoende aandacht heeft voor IB&P en/of de rol van de CISO en de PO.

2 INFORMATIEBEHOEFTE GS

Vragen aan uzelf:

- Hoe weet ik dat ik voldoende 'in control' ben wat betreft IB&P?
- Word ik tijdig betrokken bij dilemma's en afwegingen?

Vervolgvragen aan de CISO/PO:

- Wat zijn onze kritische processen ('kroonjuwelen')?
- Welke informatiebeveiligings- (CISO) of privacyrisico's (PO) zijn er? Waar moeten wij op anticiperen?
- Welke maatregelen adviseert u om deze risico's te beheersen en waarom?
- Heeft u voldoende toegang tot de kennis en ervaring van andere CISO's / PO's en de IBD?

Informatie die u kunt delen met de CISO/PO:

- Van welke risico's ligt u wakker?
- Wanneer wilt u geïnformeerd worden en over welke onderwerpen of situaties?
- Hoe bereiken wij elkaar (bellen, sms, tekst, e-mail, memo, etc.)?

3 UITBESTEDING ICT

Gemeenten besteden (een deel) van hun ICT uit bij leveranciers of grotere buurgemeenten. Uit interviews met GS in 2021 bleek dat:

- Veel op basis van vertrouwen is geregeld en minder op contracten.
- Afspraken over verantwoordelijkheden onvoldoende zijn vastgelegd.
- Te weinig controles op governance en IB&P worden uitgevoerd.
- Gemeenten onderling vaak zeer informeel handelen in hun rollen als opdrachtgever en opdrachtnemer.

In het kader van IB&P is het cruciaal dat de governance van middelen, mensen en systemen helder in kaart is gebracht. De taakverdeling moet duidelijk zijn, zeker in geval van incidenten en verstoringen. Oefenen met actuele uitwijk- en calamiteitenplannen helpt. Weet ook wie verantwoordelijk is voor de schade als gevolg van een IB&P-incident.

3 UITBESTEDING ICT

Wat u als GS wilt weten:

- Hoe heeft uw gemeente de ICT-governance geregeld? Zit u als gemeente achter het stuur?
- Welke afspraken zijn er gemaakt over verantwoordelijkheden en ondersteuning?
- Wat betekent het voor uw gemeente (en dus voor uw inwoners en bedrijven) als er een grootschalig incident is bij alle klanten van uw leverancier?

Vragen:

- Zijn de IB&P risico's voorafgaand aan de uitbesteding of inkoop van ICT-middelen in kaart gebracht?
- Hoe (en waar) zijn de afspraken met onze leveranciers contractueel vastgelegd?
- Wat zijn de afspraken over het melden van incidenten door de leverancier aan ons?
- Wanneer was het laatste incident en wat was er aan de hand?
- Wat zijn de continuïteitsrisico's die de gemeente nu of op korte termijn bedreigen?
- Wat zijn de verantwoordelijkheden in geval van een incident of een crisis bij de leverancier en/of bij de gemeente?
- Hoe vaak controleren wij of onze leveranciers voldoen aan de contractuele afspraken?
- Hebben wij nog de kennis en kunde in huis om IB&P te bewaken bij de uitbestede diensten?

4 INCIDENTEN EN CONTINUÏTEIT

- Incidenten komen altijd voor. Het is niet de vraag of uw gemeente last krijgt van een serieus incident, maar wanneer.
- Als GS wilt u weten hoe uw gemeente is voorbereid op incidenten. U wilt weten welke maatregelen uw organisatie heeft genomen, zodat dat de continuïteit van de dienstverlening aan de burger is gewaarborgd in geval van een incident.
- Als GS spreekt u regelmatig met de CISO, de FG en de PO, waar incidenten en waarborging van continuïteit aan bod komen. U denkt samen na over (bestuurlijke) dilemma's bij een incident.
- Een cyberincident kan ontaarden in een (fysieke) crisis, die consequenties kan hebben voor de (met name kwetsbare) burgers in uw gemeente. Oefen daarom regelmatig met het uitwijk- of calamiteitenplan. U kunt gebruikmaken van de ondersteuningsproducten van de IBD, zoals de aanpak Verhogen Digitale Weerbaarheid (VDW). Module 1 behandelt processen en beveiligingsmaatregelen die gemeenten ten minste op orde zouden moeten hebben.

4 INCIDENTEN EN CONTINUÏTEIT

Stel de CISO de volgende vragen over de basis beveiligingsprocessen:

- Hoe snel en goed kunnen wij reageren op incidenten (incidentmanagement)?
- In hoeverre kennen wij ons ICT-landschap en weten we wat van wie is (configuratiemanagement)?
- Kennen we de kwetsbaarheden van wat we in huis hebben aan ICT-middelen? En weten we in hoeverre ze recent zijn geüpdatet (patchmanagement)?
- Kunnen we beheerst omgaan met wijzigingen in de ICT infrastructuur (wijzigingsbeheer)?

Stel de CISO de volgende vragen over de beveiligingsmaatregelen:

- Zijn het incidentmanagementplan en de continuïteitsplannen op orde?
- Wanneer zijn deze continuïteitsplannen voor het laatst geüpdatet?
- Wanneer zijn deze continuïteitsplannen voor het laatst geoefend en wie waren daarbij betrokken?

5 GS EN IB&P

Inwoners en bedrijven moeten ervanuit kunnen gaan dat de gegevens die zij beschikbaar stellen aan de gemeente op een veilige en rechtmatige, behoorlijke en transparante manier verwerkt worden. De regels daarvoor staan beschreven in de Algemene verordening gegevensbescherming (AVG).
In deze context hangen informatiebeveiliging en privacy nauw met elkaar samen. Privacy gaat over het vertrouwelijk omgaan met persoonsgegevens. Informatiebeveiliging gaat over de beschikbaarheid, integriteit en vertrouwelijkheid van alle informatie, dus ook persoonsgegevens. Zowel informatiebeveiliging als privacy vragen om een risico-gedreven aanpak.

Als GS is het uw verantwoordelijkheid:

- dat alle processen en systemen en daarbij behorende middelen onder de verantwoordelijkheid vallen van een afdelingshoofd, proceseigenaar, procesbeheerder of systeemeigenaar;
- te sturen op concernrisico's ten aanzien van informatieveiligheid en privacy;
- dat informatiebeveiligingsonderwerpen onderdeel zijn van de P&C-gesprekken en dat risico's worden opgenomen in de auditplannen.

5 GS EN IB&P

Wat u als GS wilt weten: is uw organisatie goed voorbereid?

- Hebben we een functionaris gegevensbescherming (FG) een privacy officer (PO) en een chief information security officer (CISO)?
- Spreek ik deze functionarissen op vaste momenten (bijvoorbeeld maandelijks)?
- Staat IB&P standaard op de agenda van het managementteam?
- Worden er risicoanalyses en DPIA's uitgevoerd bij nieuwe projecten of de aanschaf van systemen en applicaties? Hoe wordt het implementeren van maatregelen gemonitord en getoetst?
- Wat is ons ENSIA-resultaat en wat zegt dit over de feitelijke veiligheid?
- Hoe staat het met het invoeren van basismaatregelen en basisprocessen van de aanpak Verhogen Digitale Weerbaarheid, module 1 (VDW1) van de IBD?
- Hoe ver zijn we met de toepassing van de AVG? Gebruiken we het Borgingsproduct van de IBD om dit te monitoren?
- Van welke IB&P knelpunten gaan we op korte of lange termijn last krijgen?
- Gebruiken we de Integrale Risico en Privacy Analyse tool (IRPA) van de IBD voor het uitvoeren van risicoanalyses en DPIA's?
- In hoeverre begrijpen medewerkers de beginselen van de AVG en kunnen zij die toepassen in hun dagelijks werk?

6 SAMENWERKINGSVERBANDEN

Gemeenten voeren hun taken en processen steeds vaker uit in samenwerkingsverbanden. Dit heeft voor- en nadelen.

Wanneer met een taak of proces ook een deel van de verantwoordelijkheid wordt uitbesteed, besteedt u ook de bijbehorende risico's en maatregelen uit. Dit kan efficiencywinst opleveren en tegelijkertijd leiden tot onduidelijkheid over wie wat doet en welke verantwoordelijkheden daarbij horen. Ook over informatiebeveiliging en privacy.

Een incident in het IB&P-domein bij een gemeente kan leiden tot een verstoring in het gehele samenwerkingsverband. Als GS wilt u daarom weten in hoeverre de verantwoordelijkheden in zo'n constructie voldoende duidelijk zijn uitgewerkt.

6 SAMENWERKINGSVERBANDEN

Als GS wilt u weten van de proceseigenaren:

- Welke (contractuele) afspraken hebben wij gemaakt of gaan we maken bij samenwerkingsverbanden aangaande IB&P?
- Welke informele afspraken hebben wij gemaakt in samenwerkingsverbanden aangaande IB&P?
- Hoe verantwoorden bestuurders van de samenwerkingsverbanden zich hiervoor?
- Doen de continuïteitsplannen recht aan de continuïteitseisen van onze gemeente?
- Is het samenwerkingsverband aangesloten bij de IBD?
- Wie zijn de eigenaren van de ICT-middelen die samenwerkingsverband gebruikt en hoe hebben die de veiligheid geregeld?

7 IS DE BASIS OP ORDE?

Onderzoek toont aan dat een aantal basisprocessen en maatregelen rond cybersecurity al direct veel bescherming geeft. Het programma Verhogen Digitale Weerbaarheid (VDW) van de IBD ondersteunt gemeenten om de basis op orde te krijgen. Deze processen horen thuis in de ICT afdeling.

Wat is de basis?

- **Configuratiebeheer.** Weten waaruit het ICT-landschap van uw gemeente is opgebouwd. Waar we het bestaan niet van weten, kunnen we niet beschermen.
- **Incidentmanagement.** Incidenten zullen altijd optreden, maar hoe beter u bent voorbereid, hoe beperkter de impact zal zijn op uw bedrijfsprocessen.
- **Patchmanagement / kwetsbaarhedenbeheer.** Alle software moet frequent worden bijgewerkt ("gepatcht") om oude en nieuwe kwetsbaarheden bij te werken. Gebeurt dit niet, dan nemen kwetsbaarheden en risico's toe.
- **Wijzigingsbeheer.** Het beheerst doorvoeren van wijzigingen in software en systemen verkleint de kans op verstoring van gemeentelijke processen.
- **Monitoring en respons (M&R).** Wat onzichtbaar is kunt u niet oplossen. M&R logt alle activiteiten in uw ICT-infrastructuur. Het is een van de belangrijkste tools om hacks en foutmeldingen op te sporen voor zaken echt uit de hand lopen.

Deze vragen kunnen worden gesteld aan het hoofd I&A / ICT!

7

IS DE BASIS OP ORDE?

?

Monitoring en respons

- Hebben wij monitoring en respons ingericht? Wie voert dat uit?
- Hoeveel meldingen hebben we ontvangen?

Incidentmanagement

- Hoeveel incidenten hebben we de afgelopen maanden gehad?
- Hoe snel worden incidenten opgelost na ontdekking?

Configuratiebeheer

- Wanneer is er voor het laatst geïnventariseerd wat we in huis hebben aan ICT-middelen?
- Hebben we licenties voor al onze software? Hoeveel licenties hebben we?
- Hoe scannen we op aanwezige configuraties?

Kwetsbaarhedenbeheer

- Als de IBD een high/high melding verstuurt, hoe snel reageren we daar dan op?
- Zijn er patches, die om wat voor reden ook, niet zijn geïnstalleerd? Welk risico lopen we?

Configuratiebeheer

- Wanneer is er voor het laatst geïnventariseerd wat we in huis hebben aan ICT-middelen?
- Hoe scannen we op aanwezige configuraties?

Wijzigingsbeheer

- Hebben we wijzigingsbeheer ingericht ? Hoeveel verstoringen hebben we gehad door onjuist doorgevoerde wijzigingen?

U kunt natuurlijk ook gewoon vragen of deze processen ingericht zijn.

8 GS, PRIVACY & DE AVG

Waarom is privacy een belangrijk onderwerp voor gemeenten en hoe zit het met de AVG?

Burgers moeten erop kunnen vertrouwen dat de gemeente rechtmatig, behoorlijk en transparant met hun persoonsgegevens omgaat.

- Ze hebben rechten t.a.v. de gegevens die de gemeente verwerkt. Daarop kunnen zij formeel aanspraak maken.
- Burgers moeten geïnformeerd worden over wat de gemeente met hun persoonsgegevens doet.
- Voordat een gemeente begint met een nieuw proces waarin persoonsgegevens verwerkt worden, moet ze toetsen of de verwerking aan de wettelijke kaders voldoet: Mag dit? Is het noodzakelijk? Kan het met minder? Is de beveiliging goed geregeld? En is de verwerking voor de burger transparant en voorzienbaar?
- Bestaande processen die risicovol zijn, moeten periodiek worden getoetst.
- Er moet een register van verwerkingen zijn, waarin per doel staat hoe persoonsgegevens worden verwerkt. In het privacybeleid legt de gemeente vast hoe ze borgt dat de verwerking van persoonsgegevens aan de wettelijke kaders voldoet.
- Het is belangrijk om zicht te hebben op alle partijen die namens de gemeente persoonsgegevens verwerken. Met deze partijen moeten afspraken zijn gemaakt. Het nakomen daarvan moet worden gemonitord en de verantwoordelijkheden, ook bij incidenten, moeten duidelijk zijn.

Mocht een incident zich dan toch voordoen, dan is door deze maatregelen nagenoeg uitgesloten dat het incident is veroorzaakt door onrechtmatig en onbehoorlijk bestuur.

8 GS, PRIVACY & DE AVG

?

- Is voor onszelf en voor onze inwoners en bedrijven duidelijk hoe de gemeente omgaat met persoonsgegevens van burgers? Wat voor gemeente willen wij zijn op dat gebied?
- Is privacy geborgd in al onze werkprocessen? Kunnen wij dit ook aantonen?
- Hoe staat het met de implementatie en naleving van de AVG binnen de organisatie? Gebruiken we het IBD- Borgingsproduct om dit te monitoren?
- Is er, over de hele breedte van de organisatie, voldoende aandacht voor het onderwerp privacy?
- Is er een veilige cultuur om incidenten met persoonsgegevens te melden?
- Hoe faciliteer ik als GS het goede bestuurlijke gesprek over privacy?
- Welke kansen zie ik als we de uitgangspunten van de AVG vertalen naar efficiënte bedrijfsvoering?
- Welke incidenten hebben zich voorgedaan en wat hebben we daarvan geleerd?
- Worden er risicoanalyses en DPIA's uitgevoerd bij nieuwe projecten en de aanschaf van systemen en applicaties? Hoe wordt het implementeren van maatregelen gemonitord en getoetst?
- Is bijvoorbeeld ook rekening gehouden met privacy bij onze smart city oplossingen en word ik hierover voldoende geïnformeerd?
- Zijn er knelpunten waarvan ik moet weten?

9 DE PROCESEIGENAREN

We hebben een CISO, PO en FG, dus alles is opgelost. Niets is minder waar!

- Binnen gemeenten denkt men vaak dat de verantwoordelijkheid voor informatiebeveiliging en privacy in zijn totaliteit bij de CISO, de PO en de FG ligt. Dit is onjuist. De proceseigenaar is verantwoordelijk voor het waarborgen van de integriteit, vertrouwelijkheid en beschikbaarheid van de informatie binnen zijn of haar proces.
- De gemeente kent proceseigenaren. Zij zijn verantwoordelijk voor één of meerdere processen, vaak binnen één domein zoals werk en inkomen. Zij hebben doorgaans oog voor het proces, de bemensing en de middelen. De proceseigenaar is echter ook verantwoordelijk voor de beveiliging en bescherming van de informatie die binnen hun proces wordt verwerkt en opgeslagen.
- Zij zijn ook verantwoordelijk voor het identificeren en managen van de IB&P risico's binnen hun proces, en passende informatiebeveiligings- en privacy beschermende maatregelen om deze risico's te beperken.

9

DE PROCESEIGENAREN

?

Als GS kunt u de volgende vragen stellen aan proceseigenaren om te toetsen of zij de juiste dingen doen op het gebied van informatiebeveiliging en gegevensbescherming:

- Zijn alle gegevens die binnen uw proces worden verwerkt, geïdentificeerd en geclassificeerd op basis van hun vertrouwelijkheid, integriteit en beschikbaarheid?
- Welke maatregelen heeft u genomen om de vertrouwelijkheid, integriteit en beschikbaarheid van de gegevens te waarborgen? En hoe heeft u bepaald dat deze maatregelen voldoende zijn?
- Welke beveiligingsmaatregelen zijn er getroffen om te voorkomen dat ongeautoriseerde personen toegang krijgen tot de gegevens binnen uw proces?
- Worden er regelmatig back-ups gemaakt van de gegevens die binnen uw proces worden verwerkt? En hoe wordt de integriteit van deze back-ups gewaarborgd?
- Zijn medewerkers binnen uw proces getraind in informatiebeveiliging en zijn ze zich bewust van de risico's van bijvoorbeeld phishing, social engineering en ransomware?

10 PROCESAUTOMATISERING

Procesautomatisering, wat is dat, en waarom is het belangrijk?

- Doorgaans leggen gemeenten bij IB&P de nadruk op kantoorautomatisering, procesautomatisering (PA) is minstens zo belangrijk, maar krijgt niet altijd de aandacht die het verdient. Dit wordt ook wel 'Operational Technology' (OT) genoemd, hieronder valt ook IoT – Internet of things.
- Denk bij PA aan:
  - Gebouwbeheersingssystemen, Camera systemen, verkeersregelinstallaties en -meetsystemen, bediening van sluizen en bruggen, rioolpomp gemalen, toegangssystemen, zwembadinstallaties etc.
  - Waar bij ICT de nadruk ligt op beschikbaarheid en vertrouwelijkheid, ligt bij PA de nadruk op veiligheid (safety) en continuïteit.
- Het is van belang te weten welke PA de gemeente heeft, wie ervoor verantwoordelijk is en of de risico's goed worden gemanaged. Systemen die dingen besturen in de gemeentelijke buitenruimte kunnen bij falen grote gevolgen hebben voor burgers.

10 PROCES AUTOMATISERING?

Als GS kunt u de volgende controlevragen stellen aan proceseigenaren om te toetsen of zij de juiste dingen doen voor de beveiliging van PA:

- Zijn alle PA systemen van de gemeente bekend en geregistreerd?
- Zijn voor alle PA systemen de eigenaren bekend?
- Zijn voor de PA systemen de risico's geïnventariseerd?
- Zijn de maatregelen om deze risico's te beheersen geïmplementeerd?

11 RISICOMANAGEMENT

Risicomanagement, wat is dat, en waarom is het belangrijk?

- Risicobeheersing is noodzakelijk om risico's voor organisatie, burgers en bedrijven te voorkomen.
- Risico's zijn niet altijd evident. Daarom moeten ze actief zichtbaar worden gemaakt via risicoanalyses met de IRPA tool van de IBD. Bij risicovolle verwerkingen van persoonsgegevens is dat zelfs verplicht (dmv DPIA's).
- Minimale IB normen staan in de BIO en P normen in de AVG. Minder IB maatregelen nemen kan alleen gemotiveerd, minder P maatregelen waardoor privacy risico blijft bestaan is geen optie.
- Risicoanalyses helpen de gemeenten om risico's te prioriteren. Risico's met een grote kans en een grote impact moeten gemanaged worden. Bij risico's met een kleine impact en kleine kans kan de gemeente een kosten-baten-afweging maken. Daarover moet het bestuur zich kunnen verantwoorden.
- Het is van belang te monitoren of maatregelen het gewenste effect hebben.
- Omstandigheden veranderen. Risico's en maatregelen – en dus ook de risicoanalyses - moeten periodiek worden geëvalueerd.

11 RISICOMANAGEMENT

Als GS kunt u de volgende controlevragen stellen aan proceseigenaren om te toetsen of zij de juiste dingen doen in het kader van risicomanagement:

- Hoe beheersen wij de risico's?
- Hoe zorgen wij ervoor dat risicoanalyses tijdig worden uitgevoerd? (Met tijdig wordt hier bedoeld dat risico- en privacy analyses worden uitgevoerd voordat een product of dienst wordt geïmplementeerd.)
- Hebben we inzicht in onze risicovolle verwerkingen?
- Hoe monitoren wij de effectiviteit van onze maatregelen?
- Wie maakt de afweging over kosten en baten van maatregelen in onze organisatie?
- Wie accepteert de risico's waar we geen maatregelen op nemen?
- Worden de CISO, FG en PO door proceseigenaren tijdig betrokken bij beoordelen van uitgevoerde risicoanalyses en/of DPIA's?

Bezoekadres
Nassaulaan 12
2514 JS Den Haag

Postadres
Vereniging Nederlandse Gemeenten
t.a.v. Informatiebeveiligingsdienst voor gemeenten (IBD)
Postbus 30435
2500 GK Den Haag

info@IBDgemeenten.nl

070 204 55 11